State of West Virginia Office of Technology Policy:
Digital Media Protection

Issued by the CTO

1.0 PURPOSE

This policy defines standards, procedures, and restrictions for Executive Branch employees who use devices to connect to a WVOT-supported network, in order to store, back-up, relocate, or otherwise access enterprise data in a safe, secure manner.

2.0 SCOPE

This policy applies to all Departments (including Agencies, Boards, and Commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. However, the WVOT recommends that all agencies, including those excluded above, follow this procedure.

3.0 POLICY

3.1 The security safeguards may vary by device type, but in all cases must comply with the requirements set forth in this policy. This document is not all-inclusive and management has the authority and discretion to appropriately address any unacceptable behavior and/or practice not specifically mentioned herein.

3.2 For the purposes of this policy, “Digital Media” includes any state-owned media in the following categories:

3.2.1 Magnetic media, including internal and external hard disk drives, external devices containing hard disk drives, floppy disks and magnetic tape;

3.2.2 USB-based flash drives, also known as thumb drives, jump drives, or key drives;

3.2.3 Memory cards such as SD, CompactFlash, Memory Stick or any related flash-based supplemental storage media;

3.2.4 MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function;

3.2.5 PDAs, cell phones, and Smartphones with internal flash or hard drive-based memory that support a data storage function;

3.2.6 Digital cameras with internal or external memory support;

3.2.7 Removable media, such as rewritable DVDs, CDs, and floppy disks;

3.3 Employees are prohibited from using personally owned media on state-owned devices, or to store State data.

3.4 The WVOT reserves the right to disable the ability to connect removable media and USB devices to the State network.

3.5 Agencies may prohibit flash drive use at any time in order to protect data. This prohibition should be implemented through policy, training, and/or use of technical controls (e.g. port blocking control).

3.6 All media must be encrypted with WVOT-approved software, where technically possibly.

3.7 Employees are prohibited from using flash drives or portable media that do not have adequate protection mechanisms to store or transmit sensitive data (e.g., Protected Health Information, sensitive Personally Identifiable Information, Federal Tax Information (FTI)).

3.8 Employees must not uninstall or de-activate any security controls loaded onto the media device by the WVOT, or its designee.

3.9 Employees must immediately report all security incidents or suspected incidents of unauthorized data access, data loss, and/or disclosure to incident@wv.gov.

3.10 The WVOT will establish audit trails or logs in all situations it deems is warranted. The resulting records will allow tracking of the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The WVOT has the right to monitor all employee access and/or connection to the State network in order to identify and analyze unusual usage patterns or other activity.

3.11 Employees may not use removable media devices for long term data storage.

3.11.1 If a State network connection is unavailable (ex: offsite use), removable media may be used for short term data storage and back-up purposes. Users must store all data on State servers or storage (e.g. home directory or shared network drives, etc.). If in doubt, contact the WVOT Service Desk.

3.12 When content from any State information system is output to some form of media, that content and media must be handled and stored in a manner appropriate for the data.

3.12.1 Removable media must be physically protected against loss, damage, abuse, or misuse when used, stored, and in transit.

3.13 When confidential information is physically transported it shall be done so in a secure manner and only by personnel specifically authorized to do so.

3.14 Where information is transferred to media that media shall be stored securely within a controlled area, and access to that media shall be physically restricted to authorized personnel. Once information system media is no longer needed to store or transport system information it must be completely sanitized before either reuse, or destroyed before retirement.

3.15 Employees will contact an immediate supervisor and/or the Chief Information Security Officer (CISO) if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting must be made to the CISO without delay.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 DEFINITIONS

6.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

6.2 Chief Information Security Officer (CISO) – Person designated by the CTO to oversee Information Security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

6.3 Federal Tax Information (FTI) -- FTI may consist of returns or return information and may contain personally identifiable information (PII). FTI is any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information.

6.4 Legally Protected Data / Information – Personally identifiable information (See definition below) of any kind, such as personal, financial, academic, or health related data, which is protected by privacy and/or security laws. Protected Health Information (See definition below - e.g. medical records, diagnosis information, etc.) Laws are divided into categories, federal and state, which govern the handling of certain types of sensitive information that must be protected by those authorized to use it. PHI, PII, FTI are examples of highly sensitive and regulated data.

6.5 Personally Identifiable Information (PII) –Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.

6.6 Protected Health Information (PHI) – Information, including demographic data, that relates to: an individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. PHI includes many common identifiers (e.g., name, address, birth date, Social Security Number).

6.7 Digital Media – Digital media are any media that are encoded in a machine-readable format. Digital media can be created, viewed, distributed, modified and preserved on digital electronics devices.

6.8 Security Incident – An event characterized by unexpected and unwanted system use or behavior, breach, or unintended alteration of data.

7.0 CHANGE LOG

- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.
- 09/01/2016 – Policy Reviewed. No Edits made.